

What is claimed is:

- 1 1. A method in a computer system for restricting network address-based
2 communication by selected processes to a set of specific network addresses, the method
3 comprising:
 - 4 associating at least one selected process with at least one network address;
 - 5 determining whether an attempted network address-based communication
 - 6 of a selected process is via an associated address; and
 - 7 in response to a determination that the communication is via an associated
 - 8 address, allowing the communication to proceed.
- 1 2. The method of claim 1 further comprising:
 - 2 loading at least one selected process into computer memory; and
 - 3 storing at least one association, between the process and at least one
 - 4 network address.
- 1 3. The method of claim 1 wherein:
 - 2 associations between selected processes and network addresses are stored
 - 3 in an association table in a computer memory of the computer
 - 4 system.
- 1 4. The method of claim 3 wherein:
 - 2 the association table is stored in operating system address space.

1 5. The method of claim 1 wherein:

2 a network address-based communication comprises an attempt to

3 designate a network address to be used for subsequent

4 communication.

1 6. The method of claim 1 wherein:

2 a network address-based communication comprises an attempt to associate

3 a communication channel with a network address.

1 7. The method of claim 1 wherein:

2 a network address-based communication comprises an attempt to

3 communicate without designating a network address to be used for

4 communication.

1 8. The method of claim 1 wherein:

2 a network address-based communication comprises an attempt to establish

3 a connection to a second process.

1 9. The method of claim 1 wherein:

2 a network address-based communication comprises an attempt to transmit

3 data to a second process.

1 10. The method of claim 9 wherein:

2 the second process is executing in a computer memory of the computer

3 system.

11. The method of claim 9 wherein:

the second process is executing in a computer memory of a second computer system.

12. The method of claim 1 further comprising:

determining whether an attempted network address-based communication is via an associated address by intercepting system calls that pertain to network address-based communication.

13. The method of claim 12 further comprising:

storing object code that determines whether an attempted network address-based communication is via an associated network address; and wherein intercepting comprises replacing a pointer to a system call with a pointer to the object code, such that calling the system call causes the object code to execute.

14. The method of claim 13 further comprising:

loading an interception module into computer memory, the interception module comprising the object code.

15. The method of claim 14 wherein:

the interception module is loaded into a running operating system kernel.

16. The method of claim 13 wherein determining whether an attempted network

2 address-based communication is via an associated network address comprises:

3 examining at least one stored association to determine whether the
4 processes that called the system call is associated with at least one
5 network address; and
6 in response to a determination that the processes is associated with at least
7 one network address, determining whether the attempted
8 communication is via an associated network address.

1 17. The method of claim 1 further comprising:
2 determining whether an attempted network address-based communication
3 is via an associated address by modifying a communication
4 protocol stack so as to intercept communication protocol
5 subroutines that pertain to network address-based communication.
6
1 18. The method of claim 17 further comprising:
2 storing object code that determines whether an attempted network address-
3 based communication is via an associated network address; and
4 wherein intercepting comprises replacing a pointer to a subroutine with a
5 pointer to the object code, such that calling the subroutine call
6 causes the object code to execute.
7
1 19. The method of claim 18 further comprising:
2 loading an interception module into computer memory, the interception
3 module comprising the object code.
4
1 20. The method of claim 19 wherein:

2 the interception module is loaded into a running operating system kernel.

1 21. The method of claim 18 wherein determining whether an attempted network
2 address-based communication is via an associated network address comprises:

3 examining at least one stored association to determine whether the process

4 that called the subroutine is associated with at least one network

5 address; and

6 in response to a determination that the processes is associated with at least

7 one network address, determining whether the attempted

8 communication is via an associated network address.

1 22. The method of claim 17 wherein:

2 the communication protocol stack that is modified is a Transmission

3 Control Protocol/Internet Protocol stack.

1 23. The method of claim 1 further comprising:

2 detecting creation of a child process by a selected process;

3 associating the child process with all network addresses with which the

4 selected process is associated.

1 24. The method of claim 23 further comprising:

2 detecting creation of a child process by intercepting system calls that

3 create child processes.

1 25. The method of claim 24 further comprising:

storing object code that detects creation of a child process by a selected process, and that associates the child process with all network addresses with which the selected process is associated; and

- wherein intercepting comprises replacing a pointer to a system call with a pointer to the object code, such that calling the system call causes the object code to execute.

26. The method of claim 25 further comprising:

loading an interception module into computer memory, the interception module comprising the object code.

27. The method of claim 26 wherein:

the interception module is loaded into a running operating system kernel.

28. The method of claim 25 wherein associating comprises:

storing an association between the child processes and a network address.

29. The method of claim 1 further comprising:

associating a child process of a selected process with a single network

address with which the selected process is associated;

determining whether network address-based communication of the child

process is via the associated address; and

in response to a determination that the communication is via the associated

address, allowing the communication to proceed.

1 30. The method of claim 1 further comprising:
2 associating a child process of a selected process with at least two network
3 addresses with which the selected process is associated;
4 determining whether network address-based communication of the child
5 process is via an associated address; and
6 in response to a determination that the communication is via an associated
7 address, allowing the communication to proceed.

1 31. The method of claim 1 further comprising:
2 detecting termination of a selected process; and
3 deleting all associations between the process and network addresses.

1 32. The method of claim 31 further comprising:
2 detecting termination of a selected process by intercepting system calls
3 that terminate processes.

1 33. The method of claim 32 further comprising:
2 storing object code that deletes all associations between a selected process
3 and network addresses; and
4 wherein intercepting comprises replacing a pointer to a system call with a
5 pointer to the object code, such that calling the system call causes
6 the object code to execute.

1 34. The method of claim 33 further comprising:

2 loading an interception module into computer memory, the interception
3 module comprising the object code.

1 35. The method of claim 34 wherein:

2 the interception module is loaded into a running operating system kernel.

1 36. The method of claim 31 wherein deleting comprises:

2 deleting all associations between a selected process and network
3 addresses.

1 37. The method of claim 1 further comprising:

2 in response to a determination that the attempted communication is not via
3 an associated network address, generating an error condition.

1 38. The method of claim 37 wherein:

2 generating an error condition comprises returning an error code.

1 39. The method of claim 37 wherein:

2 generating an error condition comprises throwing an exception.

1 40. The method of claim 37 further comprising:

2 in response to generating an error condition, not allowing the
3 communication to proceed.

1 41. The method of claim 1 wherein the set consists of one network address.

1 42. The method of claim 1 wherein the set consists of at least two network
2 addresses.

1 43. A method in a computer system for restricting network address-based
2 communication by selected processes to a set of specific network addresses, the method
3 comprising:

4 associating at least one selected process with at least one network address;
5 determining whether an attempted network address-based communication
6 of a selected process is via an associated address; and
7 in response to a determination that the attempted communication is not via
8 an associated address, not allowing the attempted communication
9 to proceed.

1 44. A method in a computer system for restricting network address-based
2 communication by selected processes to specific network addresses, the method
3 comprising:
4 associating at least one selected process with at least one network address;
5 detecting an attempt by a selected processes to associate a communication
6 channel with a network address; and
7 determining whether the network address with which the selected process
8 is attempting to associate a communication channel is associated
9 with the selected process.

1 45. The method of claim 44 further comprising:

in response to a determination that the network address is associated with the selected process, allowing the communication channel to be associated with the network address.

46. The method of claim 44 further comprising:

in response to a determination that the network address is not associated with the selected process, not allowing the communication channel to be associated with the network address.

47. A method in a computer system for restricting network address-based

communication by selected processes to specific network addresses, the method comprising:

associating at least one selected process with at least one network address; detecting an attempt by a selected processes to associate a communication channel with a network address, wherein a provided value for the network address comprises a wild card; and associating the communication channel with a network address that is associated with the process.

48. The method of claim 47 wherein:

the selected process is associated with a single network address; and associating the communication channel with the single network address.

1 49. The method of claim 47 wherein the selected process is associated with
2 multiple network addresses; the method further comprising:

3 associating the communication channel with one of the multiple network
4 addresses, resulting in a communication channel-network address
5 pair;
6 establishing one communication channel per each additional one of the
7 multiple network addresses;
8 associating each established communication channel with one of the
9 multiple network addresses, resulting in additional communication
10 channel-network address pairs; and
11 associating the communication channel with the communication channel,
12 network address pairs.

1 50. A method in a computer system for restricting network address-based
2 communication by selected processes to specific network addresses, the method
3 comprising:
4 associating at least one selected process with a unique local host address;
5 detecting an attempt by a selected process to communicate with a local
6 host; and
7 designating the unique local host address associated with the selected
8 process to be used by the selected process to communicate with the
9 local host.

1 51. A method in a computer system for restricting network address-based
2 communication by selected processes to specific network addresses, the method
3 comprising:

4 associating at least one selected process with at least one network address;
5 detecting an attempt by a selected process to communicate with a second
6 process via a communication channel;
7 determining if the communication channel is associated with a network
8 address; and
9 in response to determining that the communication channel is not
10 associated with a network address, associating the communication
11 channel with a network address that is associated with the process.

1 52. The method of claim 51 further comprising:

2 in response to a determination that the communication channel is
3 associated with a network address that is associated with the
4 selected process, allowing subsequent communication via the
5 communication channel.

1 53. The method of claim 51 further comprising:

2 in response to a determination that the communication channel is
3 associated with a network address that is not associated with the
4 selected process, not allowing subsequent communication via the
5 communication channel.

1 54. A method in a computer system for restricting network address-based

2 communication by selected processes to specific network addresses, the method
3 comprising:

4 associating at least one selected process with at least one network address;

5 detecting an attempt by a selected process to establish a connection
6 between a communication channel and a second process;
7 determining if the communication channel is associated with a network
8 address; and
9 in response to determining that the communication channel is not
10 associated with a network address, associating the communication
11 channel with a network address that is associated with the selected
12 process.

1 55. The method of claim 54 further comprising:
2 in response to a determination that the communication channel is
3 associated with a network address that is associated with the
4 selected process, allowing the connection to be established.

1 56. The method of claim 54 further comprising:
2 in response to a determination that the communication channel is
3 associated with a network address that is not associated with the
4 selected process, not allowing the connection to be established.

1 57. A method in a computer system for efficiently managing communication via
2 a set of specific, multiple network addresses, the method comprising:
3 associating at least one selected process with a set of specific, multiple
4 network addresses;
5 associating a separate communication channel with each one of the
6 multiple network addresses;

7 detecting an attempt by a selected processes to receive an incoming
8 request to initiate a communication session on one of the
9 communication channels;
10 identifying a first one of the communication channels that is ready to
11 receive the incoming request; and
12 allowing reception of the incoming request on the identified
13 communication channel.

1 58. A computer program product for restricting network address-based
2 communication by selected processes to a set of specific network addresses, the computer
3 program product comprising:

4 program code for associating at least one selected process with at least one
5 network address;
6 program code for determining whether an attempted network address-
7 based communication of a selected process is via an associated
8 address;
9 program code for, in response to a determination that the communication
10 is via an associated address, allowing the communication to
11 proceed; and
12 a computer readable medium on which the program codes are stored.

1 59. The computer program product of claim 58 further comprising:

2 program code for loading at least one selected process into computer
3 memory; and

4 program code for storing at least one association between the process and
5 at least one network address.

1 60. The computer program product of claim 58 further comprising:
2 program code for determining whether an attempted network address-
3 based communication is via an associated address by intercepting
4 system calls that pertain to network address-based communication.

1 61. The computer program product of claim 58 further comprising:
2 program code for determining whether an attempted network address-
3 based communication is via an associated address by modifying a
4 communication protocol stack so as to intercept communication
5 protocol subroutines that pertain to network address-based
6 communication.

1 62. The computer program product of claim 61 further comprising:
2 program code for storing object code that determines whether an
3 attempted network address-based communication is via an
4 associated network address; and
5 program code for replacing a pointer to a subroutine with a pointer to the
6 object code, such that calling the subroutine call causes the object
7 code to execute.

1 63. The computer program product of claim 62 further comprising:

2 program code for loading an interception module into computer memory,
3 the interception module comprising the object code.

1 64. The computer program product of claim 62 further comprising:
2 program code for examining at least one stored association to determine
3 whether the processes that called the subroutine is associated with
4 at least one network address; and
5 program code for, in response to a determination that the processes is
6 associated with at least one network address, determining whether
7 the attempted communication is via an associated network address.

1 65. The computer program product of claim 58 further comprising:
2 program code for detecting creation of a child process by a selected
3 process; and
4 program code for associating the child process with all network addresses
5 with which the selected process is associated.

1 66. The computer program product of claim 65 further comprising:
2 program code for detecting creation of a child process by intercepting
3 system calls that create child processes.

1 67. The computer program product of claim 66 further comprising:
2 program code for storing object code that detects creation of a child
3 process by a selected process, and that associates the child process

with all network addresses with which the selected process is associated; and

program code for replacing a pointer to a system call with a pointer to the object code, such that calling the system call causes the object code to execute.

68. The computer program product of claim 67 further comprising:

program code for loading an interception module into computer memory,
the interception module comprising the object code.

69. The computer program product of claim 67 further comprising:

program code for storing at least one association between the child processes and a network address.

70. The computer program product of claim 58 further comprising:

program code for detecting termination of a selected process; and
deleting all associations between the process and network addresses.

71. The computer program product of claim 70 further comprising:

program code for detecting termination of a selected process by intercepting system calls that terminate processes.

72. The computer program product of claim 71 further comprising:

program code for storing object code that deletes all associations between a selected process and network addresses; and

4 program code for replacing a pointer to a system call with a pointer to the
5 object code, such that calling the system call causes the object code
6 to execute.

1 73. The computer program product of claim 72 further comprising:
2 program code for loading an interception module into computer memory,
3 the interception module comprising the object code.

1 74. The computer program product of claim 71 further comprising:
2 program code for deleting all associations between a selected process and
3 network addresses.

1 75. The computer program product of claim 58 further comprising:
2 program code for, in response to a determination that the attempted
3 communication is not via an associated network address,
4 generating an error condition.

1 76. The computer program product of claim 75 further comprising:
2 program code for, in response to generating an error condition, not
3 allowing the communication to proceed.

1 77. A computer program product for restricting network address-based
2 communication by selected processes to a set of specific network addresses, the computer
3 program product comprising:

4 program code for associating at least one selected process with at least one
5 network address;
6 program code for determining whether an attempted network address-
7 based communication of a selected process is via an associated
8 address;
9 program code for, in response to a determination that the communication
10 is not via an associated address, not allowing the attempted
11 communication to proceed; and
12 a computer readable medium on which the program codes are stored.

1 78. A computer program product for restricting network address-based
2 communication by selected processes to specific network addresses, the computer
3 program product comprising:
4 program code for associating at least one selected process with at least one
5 network address;
6 program code for detecting an attempt by a selected processes to associate
7 a communication channel with a network address;
8 program code for determining whether the network address with which the
9 selected process is attempting to associate a communication
10 channel is associated with the selected process; and
11 a computer readable medium on which the program codes are stored.

1 79. The computer program product of claim 78 further comprising:

2 program code for, in response to a determination that the network address
3 is associated with the selected process, allowing the
4 communication channel to be associated with the network address.

1 80. The computer program product of claim 78 further comprising:
2 program code for, in response to a determination that the network address
3 is not associated with the selected process, not allowing the
4 communication channel to be associated with the network address.

1 81. A computer program product for restricting network address-based
2 communication by selected processes to specific network addresses, the computer
3 program product comprising:
4 program code for associating at least one selected process with at least one
5 network address;
6 program code for detecting an attempt by a selected processes to associate
7 a communication channel with a network address, wherein a
8 provided value for the network address comprises a wild card;
9 program code for associating the communication channel with a network
10 address that is associated with the process; and
11 a computer readable medium on which the program codes are stored.

1 82. The computer program product of claim 81 further comprising:
2 program code for associating the communication channel with a single
3 network address with which the selected process is associated.

1 83. The computer program product of claim 81 wherein the selected process is
2 associated with multiple network addresses; the computer program product further
3 comprising:

4 program code for associating the communication channel with one of the
5 multiple network addresses, resulting in a communication channel-
6 network address pair;
7 program code for establishing one communication channel per each
8 additional one of the multiple network addresses;
9 program code for associating each established communication channel
10 with one of the multiple network addresses, resulting in additional
11 communication channel-network address pairs; and
12 program code for associating the communication channel with the
13 communication channel, network address pairs.

1 84. A computer program product for restricting network address-based
2 communication by selected processes to specific network addresses, the computer
3 program product comprising:

4 program code for associating at least one selected process with a unique
5 local host address;
6 program code for detecting an attempt by a selected process to
7 communicate with a local host;

8 program code for designating the unique local host address associated with
9 the selected process to be used by the selected process to
10 communicate with the local host; and
11 a computer readable medium on which the program codes are stored.

1 85. A computer program product for restricting network address-based
2 communication by selected processes to specific network addresses, the computer
3 program product comprising:
4 program code for associating at least one selected process with at least one
5 network address;
6 program code for detecting an attempt by a selected processes to
7 communicate with a second process via a communication channel;
8 program code for determining if the communication channel is associated
9 with a network address;
10 program code for, in response to determining that the communication
11 channel is not associated with a network address, associating the
12 communication channel with a network address that is associated
13 with the process; and
14 a computer readable medium on which the program codes are stored.

1 86. The computer program product of claim 85 further comprising:
2 program code for, in response to a determination that the communication
3 channel is associated with a network address that is associated with

the selected process, allowing subsequent communication via the communication channel.

87. The computer program product of claim 85 further comprising:
program code for, in response to a determination that the communication
channel is associated with a network address that is not associated
with the selected process, not allowing subsequent communication
via the communication channel.

88. A computer program product for restricting network address-based communication by selected processes to specific network addresses, the computer product comprising:

program code for associating at least one selected process with at least one network address;

program code for detecting an attempt by a selected processes to establish a connection between a communication channel and a second process;

program code for determining if the communication channel is associated with a network address;

program code for, in response to determining that the communication channel is not associated with a network address, associating the communication channel with a network address that is associated with the selected process; and

a computer readable medium on which the program codes are stored.

1 89. The computer program product of claim 88 further comprising:
2 program code for, in response to a determination that the communication
3 channel is associated with a network address that is associated with
4 the selected process, allowing the connection to be established.

1 90. The computer program product of claim 88 further comprising:
2 program code for, in response to a determination that the communication
3 channel is associated with a network address that is not associated
4 with the selected process, not allowing the connection to be
5 established.

1 91. A computer program product for efficiently managing communication via a
2 set of specific, multiple network addresses, the computer program product comprising:
3 program code for associating at least one selected process with a set of
4 specific, multiple network addresses;
5 program code for associating a separate communication channel with each
6 one of the multiple network addresses;
7 program code for detecting an attempt by a selected processes to receive
8 an incoming request to initiate a communication session on one of
9 the communication channels;
10 program code for identifying a first one of the communication channels
11 that is ready to receive the incoming request;
12 program code for allowing reception of the incoming request on the
13 identified communication channel; and

14 a computer readable medium on which the program codes are stored.

1 92. A method in a computer system for restricting network address-based
2 communication by selected processes to a set of specific network addresses, the method
3 comprising:

4 associating at least one selected process with at least one network address;
5 detecting when a selected process attempts to communicate via an
6 unassociated address;
7 not allowing the attempted communication to proceed.

1 93. A computer program product for restricting network address-based
2 communication by selected processes to a set of specific network addresses, the computer
3 program product comprising:

4 program code for associating at least one selected process with at least one
5 network address;
6 program code for detecting when a selected process attempts to
7 communicate via an unassociated address;
8 program code for not allowing the attempted communication to proceed;
9 and
10 a computer readable medium on which the program codes are stored.

1 94. A method in a computer system for efficiently managing communication via
2 a set of specific, multiple network addresses, the method comprising:
3 associating at least one selected process with a set of specific, multiple
4 network addresses;

5 associating a separate communication channel with each one of the
6 multiple network addresses;
7 identifying a first one of the communication channels that is available for
8 communication; and
9 allowing communication to proceed via the communication channel.

1 95. A computer program product for efficiently managing communication via a
2 set of specific, multiple network addresses, the computer program product comprising:
3 program code for associating at least one selected process with a set of
4 specific, multiple network addresses;
5 program code for associating a separate communication channel with each
6 one of the multiple network addresses;
7 program code for identifying a first one of the communication channels
8 that is available for communication;
9 program code for allowing communication to proceed via the
10 communication channel; and
11 a computer readable medium on which the program codes are stored.